3eHouses: A Smart Metering Pilot in UK Living Labs

S.P. Le Blond[1], *Member, IEEE,* A. Holt and P. White[2]

***Abstract* — This paper describes the technical solution to a smart metering pilot project in the UK. The 3e-Houses project is a European Union funded project to install smart metering in social housing for the purpose of capturing energy consumption data and feeding it back to the residents in a meaningful way. The aim of the project is to demonstrate up to 20% decrease in energy usage through ICT alone. The paper discusses the technical approach, practical experience from the rollout to around 100 homes, the problems encountered and the remedies applied. Particular attention is paid to the transport of data between the smart metering systems located in residential homes and a remote collection server. Finally, some preliminary energy monitoring results are highlighted.**

***Index Terms*—Smart grids, Meter reading**

I. Introduction

At time of writing, all across Europe and the world, governments are imminently rolling out smart meters on a massive scale in the hope that improved metering will drive energy efficiency and help combat climate change. For example, in the UK, the department of Energy and Climate Change (DECC) state that 53 million smart gas and electricity meters will be deployed between 2014 and 2019 [1]. Ahead of this mass implementation there have been a plethora of smart metering projects and pilots [2]–[4]. This paper reports the findings of one such study. The authors are currently working on the FP7 European Union project *3eHouses*.

The 3eHouses project is a multinational study with a budget of approximately €4M [5]. The overarching goal of the project is to inform consumers better about their energy usage through ICT, resulting in more efficient energy behaviour. It is estimated that using ICT in this way could save up to 20% of domestic energy usage. The project involves two pilots in Barcelona, Spain and Leipzig, Germany followed by two replications in Bristol, UK and Sofia, Bulgaria. All the participants are living in social housing. An extensive state of the art review was carried out in [6]. This paper firstly describes the technical design of the UK replicator of 3eHouses, then discusses the practicalities of rollout and finally highlights some early results of energy monitoring.

Smart meters are viewed as a way of improving consumer energy management and enabling suppliers to develop better methods of load control. There are three components to a successful smart meter solution, namely, advanced metering technology, user-friendly feedback and a communications infrastructure. Advanced metering systems are capable of taking frequent energy measurements, typically, at sub-minute intervals. Furthermore, readings are not limited to an aggregate consumption measurement for a household, it is possible to monitor individual appliances. Given the distributed nature of smart metering systems, there is a heavy reliance on a communications infrastructure for the reliable transport of energy data (both for data collection and participant feedback).

People are becoming increasingly interconnected due to the expansion of the Internet. The Internet, however, is a public network-of-networks. There are, therefore, a number of security issues surrounding the transport of sensitive data over it. According to [1], “Smart and advanced metering will result in a step change in the amount of data available from electricity and gas metering”. This raises privacy-intrusive issues, which may even be in breach of European human-rights legislation. It is understandable that people are concerned about the collection, transport and storage of their energy data. So although it makes sense to utilize the Internet's ubiquity for smart metering, it needs to be done in such a way that data transport is not only reliable, but secure.

II. Technical Design of UK Pilot

The requirement in 3eHouses is to monitor energy usage at a high granularity, both temporally and spatially. This usage then must be fed back to the participant using ICT. The basic technical design for one house can be seen in Fig. 1.

A. Electricity

The local sensor network predominantly consists of a number of ZigBee units made by Italian manufacturer 4noks. ZigBee is a low power wireless mesh technology based on the IEEE 802.15.4 standard [7]. The 4noks family of devices use a ZigBee based proprietary protocol operating at 2.4 GHz.

Electricity consumption is monitored at the infeed point to give the dwelling’s total usage. This 4noks e-meter takes a voltage measurement from the 230V bus at the consumer fuse box, a connection which also supplies power to the unit. The current measurement is from a Current Transformer (CT) collar which is clamped around the measured load’s live feeder. The instantaneous power consumption is then

[1]S. P. Le Blond is with the Telecommunications Research Laboratory, Toshiba Research Europe Limited, Bristol BS1 4ND, UK (e-mail: simon.leblond@toshiba-trel.com). [2]A. Holt and P. White are with IP Performance.

This work is part funded by 3eHouses, an EU ICT-PSP project.

978-1-4673-2597-4/12/$31.00 ©2012 IEEE

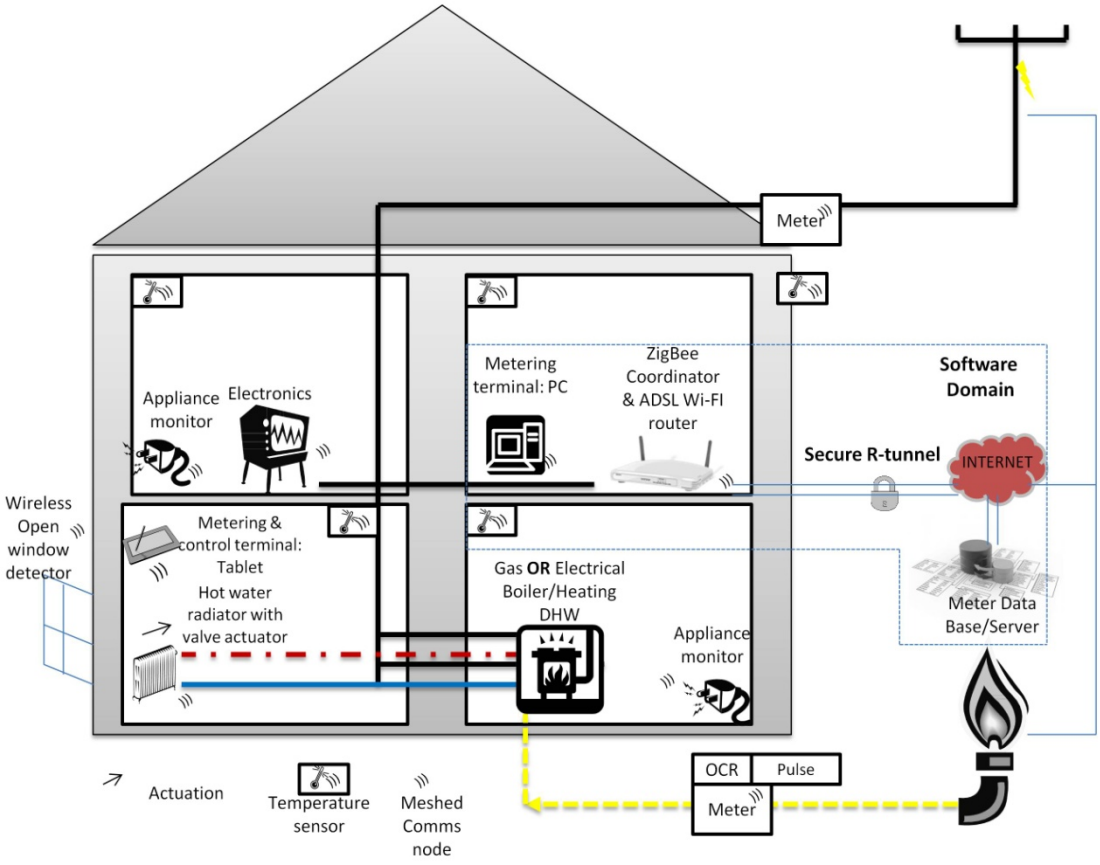

Fig. 1. Local communication solution for 3eHouses

wirelessly transmitted every 20s to the 4noks ZigBee access-point, co-located with the participant's ADSL Wi-Fi router. Another electricity meter is deployed on the circuit for the cooker, in most cases the largest overall sink of electrical energy.

Sub metering at the consumer box is also achieved using a 4noks 3 channel current sensor. Three current clamps measure the load on three different circuits. In most cases these were deployed on the upstairs and downstairs lighting loops and either the domestic hot water or an electric shower. The 3 channel device is battery powered and since it has no way of measuring voltage, instantaneous power calculations must assume a nominal voltage of 230V.

Individual appliance monitors enable wireless monitoring at the socket level. Five of these devices were deployed through the dwelling, measuring the largest loads connected through a socket. These were normally the washer/dryer, dishwasher, fridge/freezer, kettle and a 4way extension for the front room audiovisual equipment. The smart plugs transmit instantaneous load measurements to the access-point every 20s. There was some freedom given to the installers and participants regarding placement of the appliance monitors in the hope that a good variety of appliances would be measured across the study.

B. Gas

It is beyond the scope of the project to fit new gas meters: there are no suppliers or utilities amongst the UK partners and fitting new gas meters is time consuming and expensive. Therefore, a bridging device must be retrofitted to the incumbent meter. The Optical Character Recognition (OCR) unit made by Xemtec [8] can be configured to read the figures on the meter dials. This unit is glued to the face of the meter and makes an absolute reading every three minutes. It can then be configured to output in several ways, via pulse, serial, low power radio or MBus. In this case it is simply configured to produce pulses via its RJ11 port. This port is connected to the 4noks pulse logging device which then wirelessly transmits a measurement of pulses to the ZigBee access-point every 21 seconds. Careful logging of the meter characteristics are necessary to capture the units that each pulse represents. For example, in one home the resolution could be one pulse per cubic foot and another may be a hundredth of a cubic meter.

In order to actively save on gas, EQ-3 'comfort' radiator actuators were deployed in dwellings with gas space heating. These motorized devices reduce the load on the heating system by automatically adjusting radiator valves to a schedule so that, in theory, unnecessary heating can be avoided when the rooms are not in use. Wireless window shutter contacts also detect when the windows are open and signal the actuators to turn down the room's radiator during periods of ventilation. This avoids heat energy being lost directly to the surroundings. In the houses with gas heating and radiators, three of these devices were installed with two of them paired with wireless window shutters.

C. ICT

The local collector device, hereafter the *ZigBee access-point*, also made by 4noks, is IP addressable via an Ethernet link. The ZigBee access-point is connected via Ethernet to the participant's ADSL router. Using the public Internet to connect the ZigBee access-point to the remote collector presents a number of security problems, not least that of

privacy due to the absence of encryption in the IPv4 protocol. Another issue is that the participant's existing Internet connection is protected by a firewall. The firewall prevents requests being initiated from the public Internet to devices on a participant's private network (while allowing access from the private network out to the public Internet). Furthermore, it is likely that a participant's private network will use an RFC 1918 addressing scheme, (although the project has encountered some participants where the ISP has allocated public addresses to their local network). RFC 1918 network addresses are a range of Internet addresses set aside for private networks. Although public IP addresses must be unique throughout the Internet, RFC 1918 addresses can be *re-used* on different (private) networks. However, if a device with an RFC 1918 wishes to communicate with a device on the public Internet (with a unique address) it can only do so through an intermediate device running network address translation (NAT) software. Typically, this intermediate device is a participant's broadband router (which also runs the firewall). The broadband router will have a unique IP address and will map RFC 1918 addresses to this address. While this allows communication to be initiated from within the private network, out to the public Internet, it prevents the converse, as shown in Fig. 2.

The problems of the firewall and NAT can be resolved, thus:

- Add firewall rules to allow access from the public Internet.
- Use reverse NATing to statically map the router's public address and a designated TCP port to the RFC 1918 address and TCP port of the Zigeee access-point.

There are, however, downsides to this approach. Firstly, opening up firewalls to allow access from the public Internet is a security risk (and one the project was reluctant to take). There is also a logistical issue. In order to configure a participant's broadband router to add firewall rules and reverse NATing, access to the router's administration would be needed. This would require a password which the participant may not know or has forgotten. Furthermore, the participant may not want a third party accessing their broadband router. Even if obstacles over access could be overcome, the variety of broadband routers, each implementing administrative configuration procedures differently, would make the task a time consuming one.

D. Reverse Tunnel Solution

In order to overcome the problems of access between the ZigBee access-point in participant's homes and the remote collection server, a *reverse tunnel* solution was developed.

Secure Shell (SSH) is a network protocol that allows an operator on one networked machine to access the command-line on another [9]. SSH replaced terminal applications such as Telnet and RSH which are insecure because they transmit data in cleartext (including authentication passwords). SSH uses strong cryptographical methods to ensure authentication and confidentiality. A feature of SSH is the ability to perform port forwarding in order to re-direct TCP/IP sessions through encrypted tunnels. SSH can do both local and remote forwarding but it is the remote port forwarding feature that is relevant to this project and what is referred to from here on in as "reverse tunnels" (for a description of local forwarding, see [10]).

The reverse tunnel scenario is shown in Fig. 3. An embedded device (referred to as the R-tunnel) running OpenSSH is connected to the participant's network. The diagram also shows the ZigBee access-point on the participant's network.

The R-tunnel device itself is small, low power, embedded computer with a MIPS CPU running OpenWrt firmware [11]. OpenWrt is an embedded Linux distribution aimed at (but not limited to) routing wireless devices. OpenWrt enabled the building of a customised firmware image specifically for the R-tunnel application. The version of OpenWrt used was Backfire. Building a firmware image is fairly straight forward, various software packages can be selected from a menu driven system. OpenWrt includes all the necessary cross compilers for a number of platforms (including this embedded device). Once the configuration of the system is complete, a Make file is generated that builds both the root filesystem and (Linux) kernel image. These can then be flashed to the embedded device and the R-tunnel is complete.

Once the SSH connection is established, a reverse tunnel is set up that maps a TCP port on the remote collector to the TCP port on the ZigBee access-point. The monitoring software on the remote collector is now able to issue requests through the tunnel to the ZigBee access-point. The SSH command-line for creating the reverse tunnel is given below:

```
ssh -R 9100:192.0.2.10:502
ipp@203.0.113.23
```

192.0.2.10 is the address of the ZigBee access-point and 502 is the TCP port number it listens on for connection requests. 203.0.113.23 is the address of the remote collector and ipp is a valid user account on the machine. 9100 is the TCP port on the

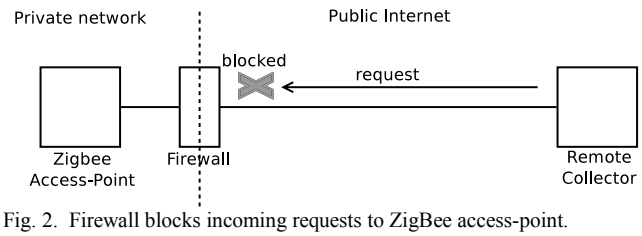

Fig. 2. Firewall blocks incoming requests to ZigBee access-point.

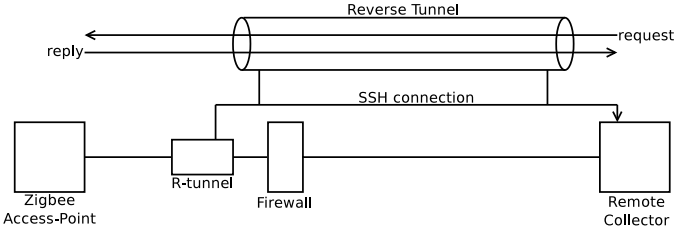

Fig. 3. The reverse tunnel allows requests from the remote collection server.

remote collector on which SSH forwards sessions to port 502 on the ZigBee access-point. Note that 192.0.2.10 and 203.0.113.23 are not the actual addresses of the ZigBee access-point or remote collector, rather they are selected from RFC 5737 address ranges reserved for documentation.

The SSH session needs to be established automatically, therefore it is not possible to use password authentication as this would require user interaction. One could use *expect* scripts to supply the password when promoted but this would mean the password would appear in the script in cleartext, which is clearly a security issue. For this reason, public key encryption for authentication is employed, which is secure and, once configured, obviates the need for user interaction. The following command will generate a public/private key pair on the R-tunnel device:

```
ssh-keygen -t rsa
```

followed by enter when prompted for a passphrase. This command generates two files in the */root/.ssh* directory, namely, *id rsa.pub* and *id rsa*, which contain the public and private keys respectively. The private key file (*id rsa*) remains on the R-tunnel device (and is given secure permissions) while the public key (*id rsa.pub*) is installed on the remote collector by appending it to the *~ /.ssh/authorized_keys2* file. On the remote collector, append the public key to the file *authorized_keys2*:

```
cat id_rsa.pub >>
~/.ssh/authorized_keys2
```

It is now possible for the SSH session (and the remote tunnel) to be established without a user having to provide a password. The smart metering monitoring software can now access the ZigBee access-point by establishing a connection to localhost (127.0.0.1) on TCP port 9100.

E. Web Portal

The energy dashboard, shown in Fig 4., is a web based portal developed by Knowle West Media Centre [12]. In Fig 4., the shoe in the centre denotes the type of house the participant lives in, while the fence surrounding the shoe is a bar chart showing hourly electrical consumption. The portal is accessed with any web browser. The project aimed to encourage access of the portal on the Toshiba AT100-100 tablet computer. The web site connects to the SQL database on the remote collection server and displays the participant's energy usage data through an intuitive and user friendly web interface. This interface is introduced to participants some time after the energy monitoring equipment has been installed so that a baseline may be established. The baseline is used to calculate the impact of ICT feedback on user energy behaviour.

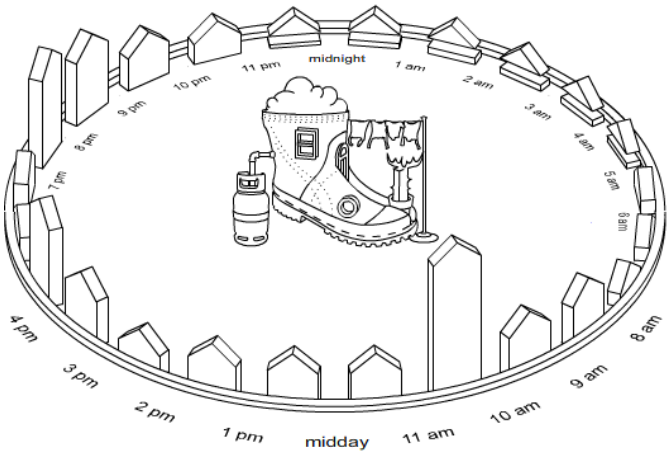

Fig.4. Web based energy monitoring portal

III. Practical Experience

Given that Wi-Fi and ZigBee both use the 2.4 GHz carrier bands the authors half anticipated problems with cross interference. However, to date no problems have been observed suggesting the protocol stacks of the respective standards are robust to the noisy area of spectrum. Moreover, ZigBee has often been dismissed as unsuitable for applications requiring transmission through thick walls due to its inferior penetration to sub GHz carriers. However, no problems with signal range have been encountered. One reason for this maybe the 4noks e-meters and appliance monitors all function as ZigBee repeaters forwarding traffic to the access-point. Each house therefore has a relatively tight pseudo mesh network.

Whereas the Spanish and German pilots are both situated in apartment blocks, the UK replicator is comprised of approximately half flats and half houses. The authors have found houses are generally more time consuming to install because there is an inherent lack of homogeneity in the infrastructure. For example, meter boxes may be inaccessible when placed high out of reach, and some may even be outside. Of those outside, the door of the meter enclosure is sometimes too close to the face of the meter, leaving little room for the Xemtec device. Moreover, the insurmountable problem with some gas meters is that there is no constantly visible display onto which to mount the OCR unit. This was a characteristic of many modern pre-pay meters, which had to be omitted from the study. Another difficulty with pre-pay customers is there are seldom historical records of their energy use to form a baseline against which to compare energy savings. Lack of historical data necessitates a period of monitoring only before feedback is given to participants.

With regards to the EQ-3 radiator actuators, it was not always trivial to determine rooms in which they are best deployed. The actuators function in a closed loop via their own proprietary protocol so they are not visible externally on the global network. This would not be desirable for the project because remote control of heating brings safety and liability problems. Nevertheless, even if heating control is local it still requires the participant's input on where the devices are best

used. However, the participant may not fully grasp the potential of the devices from the explanation given by the installer. The radiator's heating schedule must be agreed upon by both parties before the controller is programmed. The installers were given software and wireless USB dongles to expedite the programming process. Once the schedule is in place, reprogramming from the actuator without a laptop is a relatively arduous process.

In order for the R-tunnel box to work alongside the ZigBee access-point, two Ethernet ports must be available on the participant's Wi-Fi ADSL router. Otherwise a new router is required at the expense of the project budget. Whilst most participants with Internet had a Wi-Fi router, this set-up is not necessarily a given.

It is important to discuss the new equipment with the participant to ensure they have a basic understanding of its functionality. They must be aware of how to override the radiator actuators and the importance of not interfereing with the energy monitoring equipment. This challenge may be met to a greater or lesser extent depending on the participant's comfort with technical matters.

IV. Results

At time of writing, the participants had not been given access to the web interface. The results discussed herein are, therefore, showing data recorded during the baseline monitoring phase.

A. Gas

Fig. 5 shows the number of cumulative gas pulses measured over a 90 hour period during early February 2012 in dwelling 13. In this case each pulse represents one cubic foot of gas, roughly 0.3 kWh. The results show regular use of gas coinciding with daytime usage. In contrast, Fig. 6 shows a much less regular pattern over the same timescale in dwelling 22. There is some doubt as to the fidelity of these readings in the period 60 – 80 hours.

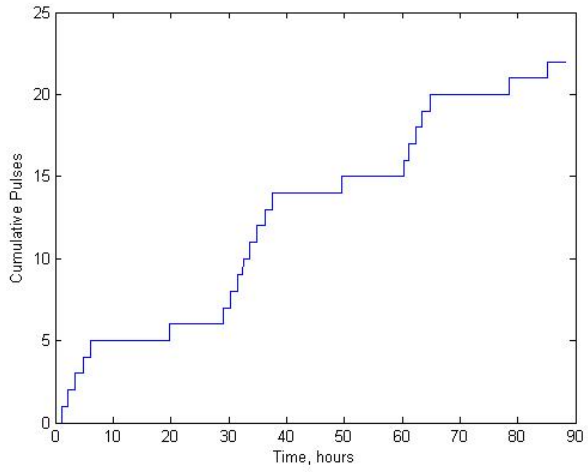

Fig. 5. Number of cumulative gas pulses measured over 90 hours, dwelling 13

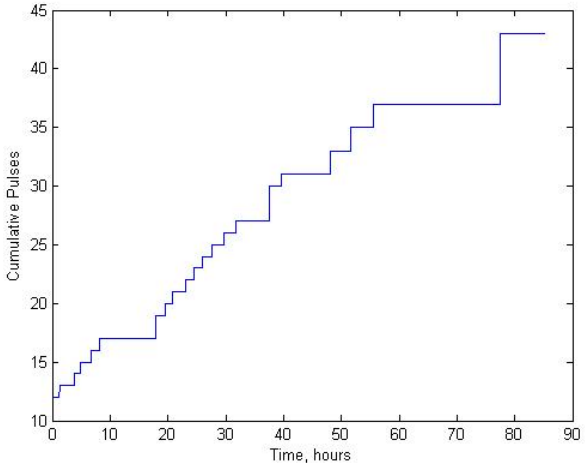

Fig. 6. Number of cumulative gas pulses measured over 90 hours, dwelling 22.

Over this period the cumulative number of pulses does not increase and then there is a step change from 37 pulses to 43. This is likely due to the OCR unit. The unit reads the meter using infrared optical character recognition. During the installation, rectangular 'regions of interest' are defined, within which lie each of the meter's characters. After the image is read the unit assigns confidence values to each character quantifying the unit's level of certainty that it has made a correct reading. During installation it is impossible to ensure confidence values are sufficiently high for every character as this would involve waiting for each of the meter's dials to make an entire revolution. In cases where the confidence value is below a certain threshold, the unit cannot be certain of the absolute value and so assumes that no change has occurred. It is likely that there is no pulse output during this period because the confidence value was too low. Encouragingly this fault is only temporary and the meter soon catches up when it is next able to make a successful absolute reading.

B. Electricity

Fig. 7 shows the electrical consumption for one dwelling over 20 hours. The sample rate on all data is 0.05 Hz. The graph's Y axis is truncated to 800 W to give a clearer view of the time series. The solid line represents the house's total consumption. By far the largest consumer of energy is the cooker, which when in use, exceeds the limit on the Y axis to around 3 kW. The next largest load is the washing machine which again, is off the scale, with consumption spikes of up to 2.5 kW. Although not used in this time window, the dishwasher later produces spikes of up to 2 kW when in use. The downstairs TV consumes some 30 W when on standby and around 180-160 W when in use. The time series produced by the TV when in use is uneven with the trace stochastically fluctuating by about 20 W. In contrast, the upstairs TV only draws about 50 W when on and a few watts when in standby. The fridge freezer is responsible for a regular pump cycle drawing around 120 W for half an hour, every two hours. Although instantaneously small compared to other kitchen

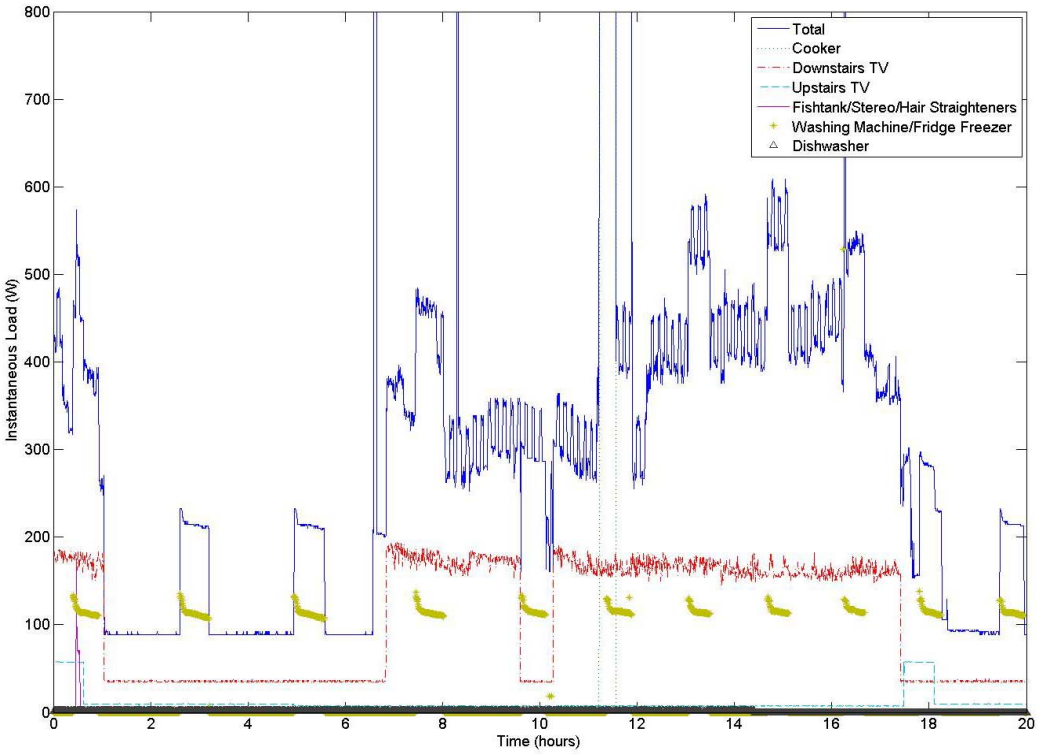

Fig 7. Electrical consumption over 20 hours, dwelling 52

appliances, this regular cycle soon amounts to a surprising amount of energy, about 0.75 kWh per day.

V. Conclusion

This paper describes the technical specification for the UK element of the 3eHouses project. Particular attention is paid to the ICT connection with details of a novel solution for transmitting local sensor values to a remote collection server. The R-tunnel solution transmits data using strong encryption and obviates the need to open up firewall rules (and configure reverse NATing) on the participant's broadband router.

In addition, some practical issues have been discussed along with some preliminary results. These early results show that the design yields both a temporally and spatially granular energy dataset. The next challenge is to establish, once the tablet web interface is introduced, to what extent energy use feedback impacts on energy efficiency.

VI. References

[1] Department of Energy and Climate Change, (2011). "Smart Meters." [Online]. Available: http://www.decc.gov.uk/en/content/cms/tackling/smart_meters/smart_meters.aspx.

[2] S. Soergel, "An Economic Smart Metering Pilot Implementation Using Standards-Based Protocols" in *Proc. 2010 Innovative Technologies for an Efficient and Reliable Electricity Supply (CITRES)*, pp. 216-219.

[3] V. Sundramoorthy, Q. Liu, G. Cooper, N. Linge and J. Cooper, "DEHEMS: A user-driven domestic energy monitoring system," *in Proc. 2010 Internet of Things (IOT)*, pp. 1-8.

[4] K. Kok, S. Karnouskos, D. Nestle, A. Dimeas, A. Weidlich, C. Warmer, P. Strauss, B. Buchholz, S. Drenkard, N. Hatziargyriou and V. Lioliou, "Smart houses for a smart grid," presented at the 20th Int. Conf. and Exhibition on Electricity Distribution (CIRED), Prague, Czech Republic 2009.

[5] 3eHouses website (2010) [Online] Available: http://www.3ehouses.eu/

[6] S. P. Le Blond, T. Lewis and M. Sooriyabandara, "Towards an integrated approach to building energy efficiency: Drivers and enablers," in *Proc. 2011 Innovative Smart Grid Technologies (ISGT Europe),* pp. 1-8.

[7] C. Gezer, M. Niccolini and C. Buratti, "An IEEE 802.15.4/ZigBee based wireless sensor network for Energy Efficient Buildings," in *Proc. 2010, IEEE 6th Int. Conf. on Wireless and Mobile Computing, Networking and Communications (WiMob),* pp. 486-491.

[8] Xemtec. (2011). "Xemtec Smart Metering Solutions." [Online]. Available: http://www.xemtec.com/

[9] D. J. Barrett and R. E. Silverman, *SSH, The Secure Shell*, O'Reilly, USA, 2001.

[10] A. Holt, "Automating the management of network devices through the command line." *Sys Admin Magazine*, Jan. 2007.

[11] P. Asadoorian and L. Pesce, *Linksys WRT54G Ultimate Hacking*, Syngress, USA, 2007.

[12] D. Watkins, Knowle West Media Centre (2011). "Daily Electric Readings." [Online]. Available: http://www.whosedata.net/dane/hourly.php.

VII. Biographies

Simon Le Blond (M'2009) studied at the University of Southampton where he graduated in 2004 with a BSc in Physics. He gained his PhD in 2011 at the University of Bath in electrical power systems. He currently works as a Research Engineer at Toshiba's Telecommunications Research Laboratory specialising in ICT for smart power systems.

Alan Holt is technical consultant at IP Performance. He has a Bachelor's degree in Computer Science and a PhD Telematics. He worked for AT&T for 13 years.

Paul White has a BA(hons) degree in Social Policy and a post graduate diploma in IT. He has been an IT professional for 25 years and is currently a Project Manager at IP Performance.